FORM PTO-1390 (Modified) (REV 11-2000) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: **182-99 PCT/US**

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR): **09/868825**

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/EP99/10141	**December 20, 1999**	**December 24, 1998**

TITLE OF INVENTION

ACTIVATABLE DOCUMENT AND SYSTEM FOR ACTIVATABLE DOCUMENTS

APPLICANT(S) FOR DO/EO/US

Staub, et al.

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include itens (5), (6), (9) and (24) indicated below.
4. ☐ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371 (c) (2))
   a. ☒ is attached hereto (required only if not communicated by the International Bureau).
   b. ☐ has been communicated by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. ☒ is attached hereto.
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))
   a. ☒ are attached hereto (required only if not communicated by the International Bureau).
   b. ☐ have been communicated by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☐ have not been made and will not be made.
8. ☒ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)).
10. ☐ An English language translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).
11. ☒ A copy of the International Preliminary Examination Report (PCT/IPEA/409).
12. ☒ A copy of the International Search Report (PCT/ISA/210).

Items 13 to 20 below concern document(s) or information included:

13. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
14. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
15. ☒ A **FIRST** preliminary amendment.
16. ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
17. ☐ A substitute specification.
18. ☐ A change of power of attorney and/or address letter.
19. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
20. ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4).
21. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
22. ☒ Certificate of Mailing by Express Mail
23. ☒ Other items or information:

    Return Receipt Postcard

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
09/868825	PCT/EP99/10141	182-99 PCT/US

24. The following fees are submitted:.

BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :		CALCULATIONS PTO USE ONLY
☐ Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO	$1000.00	
☒ International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO	$860.00	
☐ International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO	$710.00	
☐ International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4)	$690.00	
☐ International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4)	$100.00	
ENTER APPROPRIATE BASIC FEE AMOUNT =		$860.00
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☒ 30 months from the earliest claimed priority date (37 CFR 1.492 (e)).		$130.00

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	
Total claims	- 20 =	0	x $18.00	$0.00
Independent claims	- 3 =	0	x $80.00	$0.00
Multiple Dependent Claims **(check if applicable)**.			☐	$0.00
TOTAL OF ABOVE CALCULATIONS =				$990.00
☐ Applicant claims small entity status. (See 37 CFR 1.27). The fees indicated above are reduced by 1/2.				$0.00
SUBTOTAL =				$990.00
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (f)).			+	$0.00
TOTAL NATIONAL FEE =				$990.00
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) **(check if applicable).** ☐				$0.00
TOTAL FEES ENCLOSED =				$990.00
Amount to be: refunded				$
charged				$

a. ☒ A check in the amount of **$990.00** to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of _____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. **08-2461** A duplicate copy of this sheet is enclosed.

d. ☐ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Charles R. Hoffmann, Esq.
Hoffmann & Baron, LLP
6900 Jericho Turnpike
Syosset, New York 11791

Kevin E. McDermott
SIGNATURE

Kevin E. McDermott
NAME

35,946
REGISTRATION NUMBER

June 21, 2001
DATE

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: U.S. Filing of International Application PCT/EP99/10141

Applicants: Staub et al.	Examiner: N/A
Serial No.: N/A	Group Art Unit: N/A
Filed: June 21, 2001	Docket: 182-99 PCT/US
For: ACTIVATABLE DOCUMENT AND SYSTEM FOR ACTIVATABLE DOCUMENTS	Dated: June 21, 2001

Assistant Commissioner for Patents
Washington, D.C. 20231

PRELIMINARY AMENDMENT

The applicants hereby amend the above referenced application so that it is in proper form for examination.

IN THE SPECIFICATION

Please amend the specification as follows:

Page 1, after the title of the invention on line 1, insert the following:

--BACKGROUND OF THE INVENTION--

Page 2, after line 12, insert the following:

--SUMMARY OF THE INVENTION--

Page 2, after line 21, insert the following:

--BRIEF DESCRIPTION OF THE DRAWINGS--

Page 2, after line 30, insert the following:

--DESCRIPTION OF THE PREFERRED EMBODIMENTS--

IN THE CLAIMS

Please cancel claims 1-18 and add the following claims:

19. A method of using an activatable document with an at least machine-readable document number, an optical marking with a machine-readable identification and a storage field disposed on a substrate for receiving an at least machine-readable check number, wherein to complete the document to provide an authenticity certificate the check number is produced as the result of a cryptographic operation with at least two parameters, the document number and the identification, and a first secret key, only when the document is put into circulation, and is written into the storage field, and that after the document is put into circulation the authenticity of the authenticity certificate is checked by means of the check number read out of the storage field and at least the parameters read on the authenticity certificate of the cryptographic operation by means of a second key different from the first key.

20. The method as set forth in claim 19, wherein the machine-readable identification is optically read out of optical-diffraction structures of the optical marking.

21. The method as set forth in claim 19, wherein an at least visually readable, individual code related to a person is written into a check field on the substrate.

22. The method as set forth in claim 19, wherein for activation of the document the check number is written in at least machine-readable characters into the storage field arranged on the substrate.

23. The method as set forth in claim 19, wherein the check number is written into the storage field of a memory of a microchip located in the substrate and that after the activation procedure the storage field is so blocked that the content of the storage field, once written in, can no longer be altered electronically.

24. The method as set forth in claim 19, wherein the magnetically readable check number is written in a magnetic strip arranged on the substrate with the storage field.

25. The method as set forth in claim 19, wherein the check number is written at least into a part of the storage field of an optical information carrier arranged on the substrate and that after the activation procedure the check number is optically read out of the optical information carrier which can no longer be altered in the storage field.

26. The method as set forth in claim 25, wherein the identification is written into another part of the optical information carrier.

27. A system for activatable documents comprising:

a document, wherein arranged on a substrate of the document is an at least machine-readable document number, an optical marking with a machine-readable identification and a storage field for receiving an at least machine-readable check number,

a validation device comprising a transport device for receiving the document without a check number, a computing unit with an input keyboard, a recording means and an optical reader for mechanically reading off the identification, wherein the recording means, the input keyboard and the optical reader are connected to the computing unit, the computing unit is programmed for cryptographic operations with a first secret key for producing the check number by encryption of at least two parameters, the document number and the identification which is read off by the optical reader, and the recording means is adapted to write the produced check number into the storage field so that upon being put into circulation the document is completed

with the check number to provide an authenticity certificate, and

a verifier comprising a computing unit adapted for cryptographic operations with a second key, the optical reader for machine reading of the identification and a receiving means for aligning the authenticity certificate to be checked in the machine reading operation, wherein the computing unit is connected at least to the input keyboard, to a display and to reading-off means and is adapted for the authenticity checking operation by means of the cryptographic operation with the second key to check the relatedness at least of the numbers recorded on the authenticity certificate, the check number and the parameters used for producing the check number, and which has the display for representing the result of the authenticity check and/or a signal line for the delivery of a permission signal.

28. The system for activatable documents as set forth in claim 27, wherein the verifier has an input keyboard for manual input of a personal identification number (PIN) for enablement of the verifier and that the verifier is adapted to check the personal identification number of the user.

29. The system for activatable documents as set forth in claim 27, wherein the verifier has an input keyboard connected to the computing unit for manual input of the parameters for the cryptographic operation to the computing unit, wherein the parameters include at least the document number and the check number.

30. The system for activatable documents as set forth in claim 27, wherein the verifier has at least one reading unit connected to the computing unit for manual input of the parameters for the cryptographic operation to the computing unit, wherein the parameters include at least the document number and the check number.

31. The system for activatable documents as set forth in claim 27, wherein the validation device has an input keyboard connected to the computing unit for manual input at

least of the document number to the computing unit.

32. The system for activatable documents as set forth in claim 27, wherein the validation device has a reading unit connected to the computing unit for manual input of the document number to the computing unit.

33. The system for activatable documents as set forth in claim 27, wherein the validation device is adapted for the input of an individual code related to a person, by means of the input keyboard, that the validation device includes a recording means in the validation device for writing the code into the check field, and that the code is one of the parameters for producing the check number in the validation device or for the authenticity check in the verifier.

34. The system for activatable documents as set forth in claim 27, wherein the computing unit in the validation device is such that upon encryption of the check number a personal identification number of an authorized person which is inputted by way of an input keyboard is incorporated as a parameter for production of the check number and that the verifier produces the permission signal in the computing unit only when in the authenticity checking procedure the personal identification number is incorporated by way of the input keyboard of the verifier in the computing unit as a parameter of the cryptographic operation.

35. The system for activatable documents as set forth in claim 27, wherein at least one validation device and at least one verifier are connected by way of a network to a central computer for bidirectional data exchange.

36. The system for activatable documents as set forth in claim 27, wherein the at least one verifier is connected by way of a signal line to a service apparatus and that the service apparatus is adapted to enable a service by means of the permission signal sent to the service apparatus by way of the signal line.

REMARKS

Applicants submit that the application as amended is now in the proper form and respectfully request early examination.

Respectfully submitted,

Kevin E. McDermott
Registration No.: 35,946
Attorney for Applicants

HOFFMANN & BARON, LLP
6900 Jericho Turnpike
Syosset, New York 11791
(516) 822-3550

136159_1.DOC

Activatable document and system for activatable documents

The invention relates to an activatable document as set forth in the classifying portion of claim 1 and a system for activatable documents as set forth in the classifying portion of claim 9.

Such activatable documents can be used for personal identifications such as for example bank checks, passes, identity cards, subscriptions, tickets, health cards, credit cards, IC-cards, electronic purses (smart cards), value-bearing documents or stocks and shares and so forth. Such a system which uses activatable documents can be used in particular in relation to authenticity checks and/or owner checks in respect of the documents.

Visually easily recognisable holograms and other diffraction structures are used for safeguarding the stated documents, in which case they are mostly non-detachably connected to the substrate of the document, in the form of labels comprising a plastic laminate for protecting the structures which have the optical-diffraction effect (EP 0 330 738 A1). In themselves such documents have a very high standard of safeguard in relation to forgery or falsification.

EP 0 713 197 A1 discloses a data carrier in card form with an electronic circuit integrated into the card body and an optical marking, wherein the content of the electronic circuit is linked to the information of the optical marking. The optical markings used can be for example characters applied with ink such as a bar code or script characters, or structures which have an optical-diffraction effect, as in CH 653 161 A5, EP 0 366 858 A1, EP 0 718 795 A1, EP 0 883 085 A1 and so forth. The specifications referred to also describe embodiments of reading and writing apparatuses for the optical markings.

Finally US No 3 833 795 describes safeguarding the authenticity of serially numbered documents (banknotes, stocks and shares). Such a document bears two number fields, one being provided for continuous numbering of the documents, being the identity number, while the other is a check number which is selected randomly upon issue and which is

recorded in a centrally held list. An issued document is checked by reference to the external list or by means of a list algorithm, in which case a reading device firstly reads off the identity number and the check number and then compares the check number of the identity number on the document to the check number found by the reading device by means of the external list or the list algorithm. That document however is not protected from copying.

A major problem however arises in connection with the security of documents in the period from manufacture up to transfer of the document to the authorised person, as in that period the documents can be stolen in the course of transport, in order to supply unauthorised persons with those documents.

The object of the present invention is to safeguard documents which are inexpensively produced in large numbers and which are protected from copying, in such a way that the authenticity features thereof are completed only upon being brought into circulation and the authenticity features can be easily and inexpensively checked by machine.

In accordance with the invention that object is attained by the features recited in the characterising portions of claims 1 and 9. Advantageous configurations of the invention are set forth in the appendant claims.

Embodiments of the invention are described in greater detail hereinafter and illustrated in the drawing in which:

Figure 1 shows a document,

Figure 2 shows an activated document,

Figure 3 shows an IC-card as a document,

Figure 4 shows an information strip,

Figure 5 shows a system,

Figure 6 shows a validation device, and

Figure 7 shows a verifier.

In Figure 1 reference 1 denotes a document, reference 2 denotes a document number, reference 3 denotes an optical marking, reference 4 denotes a storage field, reference 5 denotes a check field and reference 6

denotes a substrate. The document 1 has a substrate 6 of paper, plastic non-woven fabric, plastic foil, a laminate structure of plastic, lacquers and/or paper and so forth. The two surfaces of the substrate 6 can be printed upon, as is usual in the case of bank checks, passes, identity cards, subscriptions, tickets, health cards, credit cards, IC-cards, electronic purses (smart cards), value-bearing documents or stocks and shares, banknotes and so forth, and have at least on one side the at least machine-readable document number 2. The document number 2 can be applied to the substrate 6 in clear text and/or in the form of a bar code in known manner using normal, fluorescing or magnetic ink. Characters such as a bar code, script characters or the like, or structures having an optical-diffraction effect, can be used for the optical marking 3, being applied for example with normal, fluorescing or magnetic ink or produced by perforation of the substrate 6. The digital marking 3 includes digital information, an identification 7. Use of the optical marking 3 with structures having an optical-diffraction effect is of particular advantage, because of its high level of safeguard in relation to forgery and copying. They are known from above-mentioned specifications CH 653 161 A5, EP 0 366 858 A1, EP 0 718 795 A1 and so forth and are suitable in particular for machine reading of an identification 7 contained in the optical-diffraction marking 3. The identification 7 contains items of information about the nature of the document, the document series and so forth, but not about the document number 2 which identifies the document 1 within a series, that is to say the documents 1 of a series can be inexpensively produced and differ only by virtue of the document numbers 2 which are applied for example by printing. The size of the optical marking 3 is determined by the identification 7 contained therein and the area required typically embraces approximately 1 mm^2. Extreme values in respect of that area may achieve a lower limit at 0.1 mm^2 and an upper limit at 1 cm^2. The optical marking 3 can also be provided in a visually invisible fashion in a transparent foil in accordance with CH 653 161 A5 or may also be inconspicuously concealed within a hologram or an optical-diffraction pattern, a security feature 8, for example in accordance with CH 659 433 A5. The security feature 8 serves

to identify the document 1 for the man in the street and has a highly conspicuous action on the document 1.

The storage field 4 and the check field 5 remain empty for the purposes of delivery to the persons bringing the document into circulation (points of sale, points of issue, bank clerks etc). The document 1 is useless without a check number 9 in the storage field 4, as shown in Figure 2. When the documents are brought into circulation, the documents must attain validity by virtue of activation thereof. For example the document number 2 and the identification 7 are read off the document 1 by machine. At least those items of information are linked together in a cryptographic operation with a first secret key 10 which is present outside the document, and the check number 9 associated with the document 1 is produced from the result, and written into the storage field 4. The document 1 is only now complete and its validity can be checked on the basis of the document number 2, the identification 7 and the check number 9. With certain kinds of document, provision is also made for writing to the check field 5 during activation. The content of the check field 5 includes at least visually readable, individual information related to a person, institution, company and so forth, such as name, address, social or other insurance number, nationality, time information, amount of money and so forth. Those items of information, referred to hereinafter as the code 11, can also be processed together with the document number 2 and the identification 7 with the cryptographic operation in relation to the check number 9.

In an embodiment of the document 1, in accordance with one of the known methods the storage field 4 and/or the check field 5 is written with the check number 9 and the code 11 in machine-readable printing. This clear text, for example OCR-text, is both visually readable and also machine-readable. Instead of or together with the printing, the check number 9 can also be represented in the form of a bar code which is widespread in the retail trade.

Figure 3 shows a further embodiment of the document 1 in the form of a card (health card, credit card, IC-card, smart card, and so forth). Let into the substrate 6 is a per se known module 12 with a microchip 13, the

storage field 4 being established in the memory 14 thereof. The storage field 4 can be written only once with the check number 9 upon activation of the document 1 by means of an electronic signal sequence which is transmitted by way of a contact field 15, and there is no longer any possibility of a later change. As in the above-mentioned EP 0 713 197 A1 the signal sequence can also be transmitted by means of inductive or optical means (not shown here) to a module 12, of suitable configuration, of the document 1.

Another embodiment of the document 1 in card form has a magnetic strip 16 on the substrate 7. The check number 9 (Figure 2) and the code 11 (Figure 2), upon activation of the document 1, are recorded in magnetically encoded form in the storage field 4 or in the encoding field 5 on the magnetic strip 16. The storage field 4 has at least the magnetically readable check number 9 after activation in the storage field 4.

A further embodiment of the document 1 has in the storage field 4 an optical-diffraction information carrier 17 which is shown in Figure 4 and which is applied to the substrate 6 during the process for manufacture of the document 1, as described in above-mentioned EP 0 718 795 A1. In the unwritten condition 17', the information carrier 17 has a row of diffraction fields 18 which are arranged in pairs 19, wherein the two microscopic diffraction structures of a pair 19 differ in respect of at least one grating parameter. During the activation procedure the check number is reproduced in the form of a digital sequence on the information carrier 17, in which case in the writing operation corresponding to the bit value in each pair of one of the two diffraction fields 18 the diffraction structure is destroyed by the application of heat energy or the diffraction structure is rendered inoperative by being covered over, for example with a non-transparent cover lacquer. After activation, in each pair, one of the two diffraction structures no longer has an optical-diffraction effect, in the information carrier 17". The storage field 4 now has the check number 9 in optically easily machine-readable characters. The advantage of this information carrier 17 is that it can be written only once. Any further change in the information carrier 17 can be easily detected by machine.

In an embodiment of the document 1 the optical marking 3 and the check number 9 is produced with diffraction structures and disposed on the same information carrier 17. The advantage of this embodiment is that the operation of reading off the identification 7 and the check number 9 and the operation of writing to the information carrier 17 are effected with a single optical reader 26 in accordance with EP 0 718 795 A1. The expensive security feature 8 (Figure 1) can be omitted.

The entries 2, 9, 11, the module 12 and the magnetic strip 16 can in themselves be distributed in any desired fashion on the two sides of the document 1, in which respect it is usually only the magnetic strip 16 which is arranged on the rear side of the substrate 6.

Figure 5 shows a system 20 which is suitable for use of the above-described documents 1. The system 20 includes at least one document 1, a validation device 21 for activation of the document 1 and a verifier 22 with which an authenticity check in respect of the document 1 is to be carried out. While the validation devices 21 are set up at the small number of people bringing the documents into circulation, a multiplicity of verifiers 22 which are simple to operate and which are as far as possible autonomous must be in operation wherever such documents 1 are subjected to an authenticity check.

The documents 1 supplied by the manufacturer, with the document number 2, are stored by the persons bringing the documents into circulation, until one of the documents 1 is allocated to an authorised person, in which case the document 1 allocated to that person is completed by means of the validation device 21 by writing the check number 9 into the storage field 4, to constitute an authenticity certificate 23.

An embodiment of the validation device 21 as shown in Figure 6 includes a computing unit 24, a transport device 25 for the document, an optical reader 26 for machine reading of the identification 7 (Figure 1) on the optical marking 3 of the non-activated document 1 and a recording means 27. Further optional reading units 29 which are shown in broken line in Figure 6 permit reading-off of the document number 2 (Figure 1), the check number 9 (Figure 2) and the code 11 (Figure 2). The reading units

29 differ according to the recording technologies once selected for the system 20, which are predetermined for the document number 2, for the check number 9 and for the code 11. The transport device 25, the optical reader 26, the one or more recording means 27 and the reading units 29 are connected to the computing unit 24.

The computing unit 24 is connected by way of lines to the transport device 25, the optical reader 26 and the recording means 27, it controls those units 25, 26 and 27 and receives the items of information emitted by those units 25, 26 and 27 so that the document 1 can be read off and labelled, by machine. The computing unit 4 has at least one security module 30 which in an integrated circuit includes a microprocessor with associated memory locations. The microprocessor executes cryptographic operations and uses the first secret key 10 contained in the memory locations.

In an embodiment, the transport device 25 produces a relative movement between the document 1 on the one hand and the reading means 26, 29 and the recording means 27 on the other hand. In Figure 6 the document 1 is moved with respect to the stationary reading means 26, 29 and the recording means 27. Different per se known embodiments for sheets or for cards are known and can be used for the transport device 25. It is possible to forego an expensive transport device 25 if the optical marking 3 or the security element 8 (Figure 1) is designed in accordance with the teaching in EP 0 883 085 A1 and writing of the storage field 4 is effected manually.

The recording means 7 is adapted to write the check number 9 and the code 11 into the storage field 4 and the encoding field 5 respectively, and uses the recording procedure provided for the document 1, for example a printing, ink jet, xerographic, perforation and the like method, a writing method described in EP 0 718 795 A1 for the information carrier 17, a magnetic recording procedure or electronic storage in the memory 14 (Figure 3). The check number 9 can also be written manually into the storage field 4, with waterproof ink. The perforation method for documents 1 is described for example in German utility model No G 93 15 294.9.

The keyboard 28 is quite generally an input device for items of information consisting of digits or alphanumeric characters. The input device can also be connected to the validation device 21 by way of a connection 28' to a telephone or computer network 37 (Figure 5) and in particular the items of information forming the code 11 can be called up from a central exchange.

The reading unit 29 is adapted to the recording technology used for the document 1. The reading unit 29 is for example a clear text reader, a bar code reader and the like for visually readable characters, from which the document number 2, the check number 9 and the code 11 are composed. Those reading units 29 use a light beam to scan parts of or the entire document 1 and measure the level of intensity of the light which is scattered back from the document 1. The reading unit 29 which is suitable for the magnetically recorded information or for electronically reading out of the memory 14 is generally known.

The structure and mode of operation of the optical reader 26 and for a reading unit 29 which is capable of reading the check number 9 out of the optical information carrier 17 (Figure 4) are known for example from above-mentioned specifications CH 653 161 A5, EP 0 366 858 A1, EP 0 718 795 A1 and EP 0 883 085 A1.

In an inexpensive embodiment for the activation procedure, an operator of a non-activated document 1 visually reads off the document number 2 thereof and manually inputs the document number 2 (Figure 2) into the computing unit 24 by way of a keyboard 28. Then, the document 1 is fitted or placed into the transport device 25 which is reduced to a passage or a platform, under the optical reader 26, so that the optical reader 26 can read off the identification 7 and communicate it to the computing unit 24. The computing unit 24 encrypts the identification 7 and the document number 2 with the first secret key 10 and reproduces a digital signature, the check number 9, on a display 31. The operator now manually transfers the check number 9 into the storage field 4 on the document which now activated in that way has become the authenticity certificate 23 (Figure 5). The storage field 4 can be divided into fields for

respective characters of the check number 9 in order to facilitate machine reading of the manually entered check numbers 9.

A second embodiment has a reading unit 29 which is shown in dotted line in Figure 6 and which reads off the document number 2 by machine directly from the document 1 and passes it to the computing unit 24. The computing unit 24 encrypts at least the identification 7 and the document number 2 with the first secret key 10 to form the check number 9. The recording means 27 then transmits the check number 9 into the storage field 4 using the technology which is predetermined by the system 20.

In a third embodiment the validation device 22 is additionally provided with the keyboard 28 and the display 31 in order by way of the keyboard 28 to input the code 11, with the display 31 serving to check the code 11. The code is also transferred with the recording means 27 on to the document 1. For particularly important documents 1 the validation device 21 is designed to demand the input of a personal identification number (PIN) from the user. In one case that PIN as a permission PIN identifies the operator who is operating the validation unit 21 and in a second case as an owner PIN it identifies the document owner, in which respect, upon activation of the document 1, the owner types in his PIN by way of the keyboard 28 and in the computing unit 24 the owner PIN serves together with the code 11 or on its own as a parameter for production of the check number 9.

In a fourth embodiment of the validation device 21, instead of the optical reader 26 and the reading unit 29, a single reader 26 is so designed that it can detect both the optical marking 3 and the document number 9.

In a fifth embodiment the validation device 21 is also adapted to detect the check number 9. Thus the validation device 21 is capable of distinguishing between activated and non-activated documents 1 and in addition checking the check number 9 for the correctness thereof.

The check number 9 is the result of the cryptographic operation in the computing unit 24, a mathematical function f:

check number 9 = f(document number 2, identification 7, first secret key 10), and

check number 9 = f(document number 2, identification 7, code 11, first secret key 10).

As the systems 20 differ not only in terms of the recording technology but also in respect of the number and nature of the parameters of the cryptographic operation, for the purposes of greater ease of description hereinafter the values which are present for production of the check number 9 on the document 1 such as document number 2, identification 7, code 11 and the owner PIN which is stored separately from the document 1, are referred to as parameters of the cryptographic operation, in which respect that means at least the document number 2 and the identification 7, if need be supplemented by the code 11 and/or the owner PIN. A system 20 is thus defined by the technologies used, the nature of the document 1, the parameters of the cryptographic operation and the first secret key 10.

Neither the first secret key 10 nor the algorithm are known to the public and are issued by a certification authority in a security module 30 for insertion into the computing unit 24. After the parameters of the function f in the security module 30 are inputted into the computing unit 24 the easily replaceable security module 30 directly produces the check number 9 or an intermediate result which serves for calculation of the check number 9 in the computing unit 24.

The first secret key 10 serves both for the cryptographic operation for producing the check number 9 and also for checking the correctness of the check number 9 with knowledge of the items of information present on the document 1.

The verifier 22 in Figure 7 has the same components as the validation device 21 (Figure 6), except for the recording means 27 (Figure 6). The design configurations of the verifier 22 differ in respect of the reading units 29 which differ according to the recording technology adopted for the system 20 (Figure 5). In the inexpensive embodiment the verifier 22 includes at least one receiving means 32 for an authenticity certificate 23 to be checked (Figure 5), a computing unit 33 with the security module 30, the optical reader 26 for the identification 7, the keyboard 28 and the display 31. The computing unit 33 is connected to the optical reader 26, the keyboard 28 and the display 31. With another cryptographic operation, the

computing unit 33 checks whether the check number 9 (Figure 2) matches the parameters of the cryptographic operation, which include at least the document number 2 and the identification 7. For that purpose the computing unit 33 uses a second key 34 which is contained in the security module 30 with the corresponding algorithm. The computing unit 30 cannot implement with the other cryptographic operation any encryption procedures like the computing unit 24 (Figure 6) in the validation device 21. The use of the second key 34 which is completely different from the first key 10 affords the advantage that the difficulty of keeping the second key 34 secret, which arises out of the wide-spread use of the verifiers 22, is irrelevant in regard to the security of the system 20. The computing unit 32 represents the result of the authenticity check on the display 31.

For an authenticity check, a checker visually reads off the parameters of the cryptographic operation, at least the document number 2 and the identification 7, on the authenticity certificate 23 and the check number 9 in the storage field 4, and supplies the computing unit 33 with the read-off sequence of characters, by way of the keyboard 28. The receiving means 32 can also be a simple platform under the optical reader 26, on which the checker lays the document 1 in such a way that the optical marking 3 is in the region of the optical reader 26. The identification 7 which is machine-read passes directly into the computing unit 33. The result of the authenticity check appears on the display 31. In the simplest case, the display comprises two signal lamps in order to represent the yes/no result of the authenticity check. It is advantageous however if the display 31 displays both the check number 9 and the parameters inputted by way of the keyboard 28, and the yes/no result.

In another embodiment, the verifier outputs a permission signal by way of a signal line 35 to a services apparatus 36. Receipt of the permission signal enables the service of the apparatus 36, for example door opening, issue of money, purchase of goods, registration and so forth.

Another embodiment of the verifier 22 has a receiving means 32 in the form of a transport system for documents 1 which are in sheet or card form. Connected to the computing unit 33 is the receiving means 32 which

is controlled by the computing unit 33 and, in addition to the optical reader 26, at least one reading unit 29 for communicating items of information. The reading unit 29 reads off by machine one or more parameters of the cryptographic operation. There is no need of a keyboard 28 for this embodiment. One reading unit 29 is sufficient if the parameters of the cryptographic operation and the check number 9 on the authenticity certificate 23 are recorded using the same recording technology.

For a system 20 in which the owner PIN is used, the keyboard 28 is provided for the owner who identifies himself to the verifier 22, with the owner PIN. The owner PIN which is inputted by way of the keyboard is used in the cryptographic operation as a parameter for checking the check number 9.

As in the case of the validation device 21, identification of the checking person by means of his user PIN is also advantageous in order to set the hurdle for possible hackers into the system 20 as high as possible. Input of the correct user PIN by way of the keyboard 28 permits the computing unit 33 to identify the user and to enable the validator 22 for operation.

In regard to Figure 5 it is also to be noted that the system 20 is advantageously embedded into a bidirectional telephone or computer network 37 for data exchange between the validation devices 21 and the verifiers 22 on the one hand and a computer 39 on the other hand. The validation device 21 is connected by way of the connection 28' to the network 37 and the network 37 by way of a line 38 to the central computer 39. Besides the above-mentioned call-up of data from the central computer 39 for the code 11 (Figure 2), the network 37 also makes it possible to set up in the central computer 39 a negative list of document numbers 2 of revoked authenticity certificates 23. The verifiers 22 which are connected to the central computer 39 by way of the network 37 receive by way of a data line 40 the regularly updated negative list, being transmitted into the computing unit 33 (Figure 7). The negative list is stored in a data memory 41 (Figure 7) of the computing unit 33 so that revoked authenticity

certificates 23 are detected by the verifiers 22 even in the event of failure of the network 37.

CLAIMS

1. A document (1) having an at least machine-readable document number (2) on the substrate (6) and a storage field (4) for receiving an at least machine-readable check number (9), characterised in that an optical marking (3) with a machine-readable identification (7) is disposed on the substrate (6), and that for activation with an authenticity certificate (23) the at least machine-readable information in the storage field (4) is completed only when the document is put into circulation by writing into the storage field (4) the check number (9) forming the result of a cryptographic operation with at least two parameters, the document number (2) and the identification (7), and a first secret key (10).

2. A document (1) as set forth in claim 1 characterised in that the optical marking (2) has optical-diffraction structures and that at least a part of the optical-diffraction structures includes the machine-readable identification (7).

3. A document (1) as set forth in claim 1 or claim 2 characterised in that the substrate (6) has a check field (5) for receiving an at least visually readable, individual code (11) which is related to a person.

4. A document as set forth in one of claims 1 through 3 characterised in that the storage field (4) is arranged on the substrate (6) and that after activation the check number (9) is contained in the storage field (4) in at least machine-readable characters.

5. A document (1) as set forth in one of claims 1 through 3 characterised in that a microchip (13) is let into the substrate (6), that the storage field (4) is arranged in the memory (14) of the microchip (13), and that after activation the storage field (4) contains the check number (9) and the content of the storage field (4), once written in, cannot be altered electronically.

6. A document (1) as set forth in one of claims 1 through 3 characterised in that a magnetic strip (16) with the storage field (4) is arranged on the substrate (6), that the magnetic strip (16) contains at least the storage field (4), and that after activation the storage field (4) has the magnetically readable check number (9).

7. A document (1) as set forth in claim 1, claim 2, claim 3 or claim 4 characterised in that arranged on the substrate (6) is an optical information carrier (17, 17'), that the optical information carrier (17, 17') contains at least the storage field (4), and that after activation the optical information carrier (17, 17") which can no longer be altered in the storage field (4) has the check number (9) in optically readable characters.

8. A document (1) as set forth in claim 7 characterised in that a part of the optical information carrier (17, 17') forms the optical marking (3) and contains the identification (7).

9. A system (20) comprising at least one document (1) as set forth in one of claims 1 through 8, a validation device (21) and a verifier (22),

characterised in that

arranged in the validation device (21) is a transport device (25) for receiving the document (1), a recording means (27) and an optical reader (26) for machine reading of at least the identification (7), that the validation device (21) further includes a computing unit (24) connected to the recording means (27) and the optical reader (26) for cryptographic operations with a first secret key (10) for producing the check number (9) by encryption of at least two parameters, the document number (2) and the identification (7) which is read off by the optical reader (26), that the recording means (27) is adapted to write the check number (9) into the at least machine-readable storage field (4) for activation of the document (1) to provide the authenticity certificate (23),

that the verifier (22) has at least a computing unit (33), an optical reader (26) for machine reading of the identification (7), and a receiving means (32) for orienting an authenticity certificate (23) to be checked for the machine reading operation, that the computing unit (33) is connected to input and reading-off means (26; 28; 29) and is adapted for cryptographic operations with a second key (34), and to check the relatedness at least of the check number (9) and the parameters of the cryptographic operation, which are used for the encryption procedure and which are contained on the authenticity certificate (23), and to represent the comparison result on a display (31) of the verifier (22) and/or to produce a permission signal.

10. A system (20) as set forth in claim 9 characterised in that the verifier (22) has a keyboard (28) for manual input of a personal identification number (PIN) for enablement of the verifier (22) and that the verifier (22) is adapted to check the personal identification number of the user.

11. A system (20) as set forth in claim 9 or claim 10 characterised in that the verifier (22) has a keyboard (28) connected to the computing unit (33) for manual input of the parameters of the cryptographic operation to the computing unit (33), wherein the parameters include at least the document number (2) and the check number (9).

12. A system (20) as set forth in one of claims 9 through 11 characterised in that the verifier (22) has at least one reading unit (29) connected to the computing unit (33) for manual input of the parameters of the cryptographic operation to the computing unit (33), wherein the parameters include at least the document number (2) and the check number (9).

13. A system (20) as set forth in one of claims 9 through 12 characterised in that the validation device (21) has a keyboard (28)

connected to the computing unit (24) for manual input at least of the document number to the computing unit (24).

14. A system (20) as set forth in one of claims 9 through 12 characterised in that the validation device (21) has a reading unit (29) connected to the computing unit (24) for manual input at least of the document number to the computing unit (24).

15. A system (20) as set forth in one of claims 9 through 14 characterised in that the validation device (21) is adapted for the input of an individual code (11) related to a person, by means of the keyboard (28), that the validation device (21) includes a recording means (27) in the validation device (21) for writing the code (11) into the check field (5), and that the code (11) is one of the parameters for producing the check number (9) in the validation device (21) or for the authenticity check in the verifier (22).

16. A system (20) as set forth in one of claims 9 through 15 characterised in that the computing unit (24) in the validation device (21) is such that upon encryption of the check number (9) a personal identification number of the authorised person which is inputted by way of a keyboard (28) is incorporated as a parameter for production of the check number (9) and that the verifier (22) produces the permission signal in the computing unit (33) only when in the authenticity checking procedure the personal identification number is incorporated by way of the keyboard (28) of the verifier (22) in the computing unit (33) as a parameter of the cryptographic operation.

17. A system (20) as set forth in one of claims 9 through 16 characterised in that at least one validation device (21) and at least one verifier (22) are connected by way of a network (28', 38, 40; 37) to a central computer (39) for bidirectional data exchange.

18. A system (20) as set forth in one of claims 9 through 17 characterised in that the at least one verifier (22) is connected by way of a signal line (35) to a service apparatus (36) and that the service apparatus (36) is adapted to enable a service by means of the permission signal sent to the service apparatus (36) by way of the signal line (35).

ABSTRACT

A document (1) has on the substrate (6) at least one document number (2), an optical marking (3) with a machine-readable identification (7) and a storage field (4) for receiving a check number (9). It is only at the moment of delivery to an authorised person that the check number (9) is produced by means of a cryptographic operation from at least the document number (2), the identification (7) and a first secret key (10) and written into the storage field (4). An authenticity certificate produced in that way can be checked for its authenticity with a verifier using a cryptographic operation and the information stored on the document (1), by means of a second key.

(Figure 2)

Fig. 1:

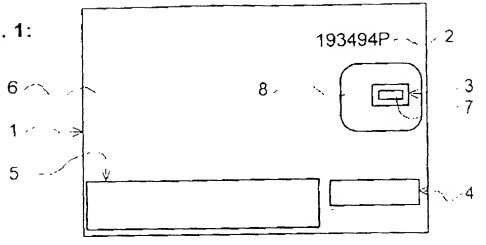


Fig. 2:

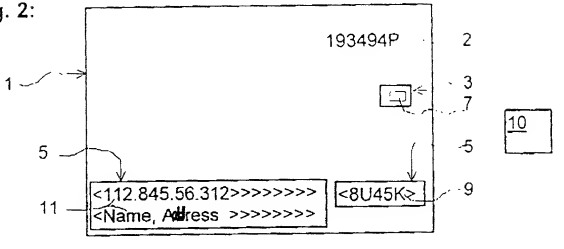


Fig. 3:

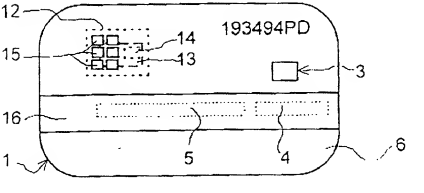


Fig. 4:

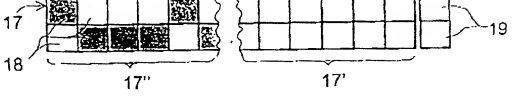


Fig. 5:

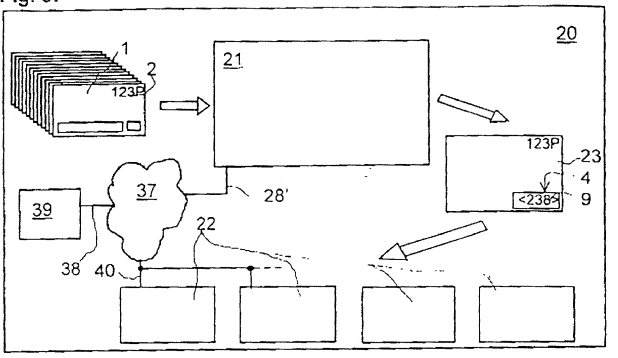

20
1
2
123P
21
123P
23
4
9
<2384
37
28'
39
22
38
40

Fig. 6:

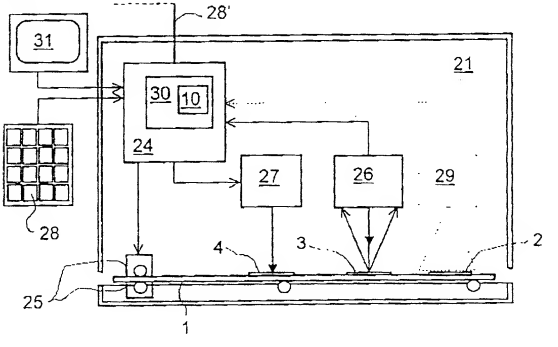
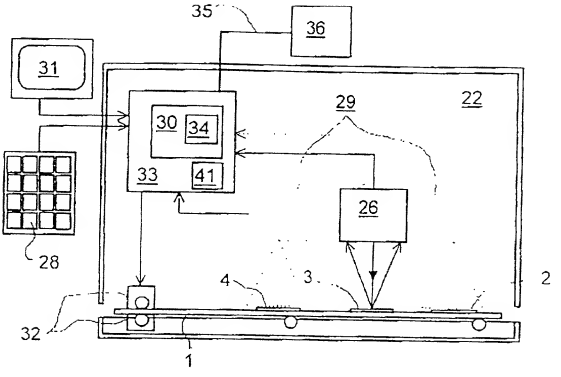

28'
31
21
30
10
24
27
26
29
28
4
3
2
25
1

Fig. 7:



P2900US/ks

Attorney's Docket No 182-99 PCT/US

PATENT

COMBINED DECLARATION AND POWER OF ATTORNEY

(ORIGINAL, DESIGN, NATIONAL STAGE OF PCT, SUPPLEMENTAL, DIVISIONAL, CONTINUATION OR CIP)

As a below named inventor, I hereby declare that:

TYPE OF DECLARATION

This declaration is of the following type: *(check one)*

- ☐ Original
- ☐ Supplemental
- ☐ Design
- ☒ National Stage PCT
- ☐ Divisional
- ☐ Continuation
- ☐ Continuation-in-Part (CIP)

INVENTORSHIP IDENTIFICATION

NOTE: If the inventors are each not the inventors of all the claims an explanation of the facts, including the ownership of all the claims at the time the last claimed invention was made, should be submitted.

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

TITLE OF THE INVENTION

the specification of which: *(complete (a), (b) or (c))*

(a) ☐ is attached hereto.

(b) ☐ was filed on _____ as
☐ Serial No. /_____ or
☐ Express Mail No. _____, as Serial No. not yet known
and was amended on _____. *(if applicable)*

(c) ☐ was described and claimed in PCT International Application No. PCT/EP99/10141
filed on _____ and as amended under PCT Article 19 on _____. *(if any)*

ACKNOWLEDGMENT OF REVIEW OF PAPERS AND DUTY OF CANDOR

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above, and that the filing of said specification, if heretofore filed, was authorized by me.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

CLAIM OF PRIORITY OF EARLIER FOREIGN APPLICATION(S) UNDER 35 U.S.C. §119(a)-(d)

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

(List prior foreign/PCT application(s) filed within 12 months (6 months for design) prior to this U.S. application.)

NOTE: Where item (c) is entered above and the International Application which designated the U.S. claimed priority check item (e), enter the details below and make the priority claim.

COUNTRY (or PCT)	APPLICATION NO.	DATE OF FILING *(Day/Month/Year)*	PRIORITY CLAIMED UNDER 35 USC §119
~~Germany~~ Switzerland	2557/98	24/12/1998	☒ YES ☐ NO
			☐ YES ☐ NO

CLAIM FOR BENEFIT OF PRIOR U.S. PROVISIONAL APPLICATION(S) UNDER 35 U.S.C. §119(e)

I hereby claim the benefit under Title 35, United States Code, §119(e) of any United States provisional application(s) listed below:

(List prior U.S. provisional applications.)

PROVISIONAL APPLICATION NO.	FILING DATE *(Day/Month/Year)*

CLAIM FOR BENEFIT OF EARLIER U.S./PCT APPLICATION(S) UNDER 35 U.S.C. 120

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) or PCT international application(s) designating the United States of America that is/are listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in such prior application(s) in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application(s) and the national or PCT international filing date of this application:

(List prior U.S. applications or PCT international applications designating the U.S. for benefit under 35 U.S.C. §120.)

U.S. APPLICATIONS		STATUS *(Check One)*		
U.S. SERIAL NO.	U.S. FILING DATE *(Day/Month/Year)*	Patented	Pending	Abandoned
0 /		☐	☐	☐
0 /		☐	☐	☐

PCT APPLICATIONS DESIGNATING THE U.S.			STATUS *(Check One)*		
PCT APPLN. NO.	PCT FILING DATE *(Day/Month/Year)*	U.S. SERIAL NOS ASSIGNED (If any)	Patented	Pending	Abandoned
PCT/EP99/10141	20/12/1999		☐	☒	☐
PCT/			☐	☐	☐

35 USC 119 PRIORITY CLAIM, IF ANY, FOR ABOVE LISTED U.S./PCT APPLICATIONS

PRIORITY APPLICATION NO.	PRIORITY COUNTRY	FILING DATE *(Day/Month/Year)*	ISSUE DATE *(Day/Month/Year)*

POWER OF ATTORNEY

As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office in connection therewith:

Charles R. Hoffmann, Reg. No. 24,102; Ronald J. Baron, Reg. No. 29,281; Gerald T. Bodner, Reg. No. 30,449; Alan M. Sack, Reg. No. 31,874; A. Thomas Kammer, Reg. No. 28,226; R. Glenn Schroeder, Reg. No. 34,720; Glenn T. Henneberger, Reg. No. 36,074; Irving N. Feit, Reg. No. 28,601; Anthony E. Bennett, Reg. No. 40,910; Gregory W. Bachmann, Reg. No. 41,593; Steven T. Zuschlag, Reg. No. 43,309; Susan A. Sipos, Reg. No. 43,128, Kevin E. McDermott, Reg. No. 35,946; Robert C. Morriss, Reg. No. 42,910; Rod S. Turner, Reg. No. 38,639; James F. Harrington, Reg. No. 44,741; Algis Anilionis, Reg. No. 36,995; Justin K. Holmes, Reg. No. 42,666; and Joseph J. Catanzaro, Reg. No. 25,837, each of them of HOFFMANN & BARON, LLP, 6900 Jericho Turnpike, Syosset, New York 11791; and Daniel A. Scola, Jr., Reg. No. 29,855; Salvatore J. Abbruzzese, Reg. No. 30,152; Kellyanne Merkel, Reg. No. 43,800; Keith R. Lange, Reg. No. 44,201; John Sopko, Reg. No. 41,321; Barry Jacobsen, Reg. No. 43,689; Gloria K. Szakiel, Reg. No. 45,149; and Mark E. Baron, Reg. No. 46,150, each of them of HOFFMANN & BARON, LLP, 1055 Parsippany Boulevard, Parsippany, New Jersey 07054.

PLEASE SEND CORRESPONDENCE TO:	PLEASE DIRECT TELEPHONE CALLS TO:
Charles R. Hoffmann, Esq. HOFFMANN & BARON, LLP 6900 Jericho Turnpike Syosset, NY 11791	Kevin E. McDermott, Esq. (516) 822-3550

DECLARATION

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further, that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

SIGNATURE(S)

Full Name of Sole or First Inventor: STAUB René

Country of Citizenship: Switzerland

Residence Address: Schmiedstrasse 6, CH-6330-Cham CHX

Post Office Address:

Date: 25/06/01 Inventor's signature

Full Name of Second Joint Inventor: TOMPKIN Wayne, Robert

Country of Citizenship: USA

Residence Address: Oesterliwaldweg 2, CH-5400 Baden CHX

Post Office Address:

Date: 25/06/01 Inventor's signature

NOTE: All above spaces identifying inventors must be completed or deleted before any inventor executes this application